

RUTTENBERG IP LAW

A PROFESSIONAL CORPORATION

1801 Century Park East, Suite 1920, Los Angeles, CA 90067

Tel: (310) 627 2270 Fax: (310) 627 2260

April 6, 2022

Hon. Joseph C. Spero
United States District Court - Northern District of California
San Francisco Courthouse, Courtroom F - 15th Floor
450 Golden Gate Ave., San Francisco, CA 94102

Re: *Cadence Design Systems, Inc. v. Syntronic AB., et al.*, Case No. 3:21-cv-3610-SI (JCS)

Dear Chief Magistrate Judge Spero:

Plaintiff Cadence Design Systems, Inc. (“Cadence”) and Defendants Syntronic AB, Syntronic US, and Syntronic Beijing respectfully submit this joint letter brief pursuant to Section 9 of the Court’s Civil Standing Order. Plaintiff hereby moves for an order to enforce its February 4, 2022 and March 3, 2022 Orders.

Plaintiff’s Portion: Defendants refuse to comply with the Court’s Orders and they are ***destroying*** key evidence. In addition to seeking the discovery here, Cadence expects to file a formal sanctions motion.

Court’s February 4 Order. In response to Cadence’s motion to compel, the Court ordered Defendants to conduct substantial searches of corporate and personal computers belonging to Defendants, their subsidiaries, and their employees, and then “fully respond” to Rgs 1-3 by March 21. (Dkt. No. 86). The Court also ordered Defendants to meet and confer to “set a deadline for completion of document production by defendants.” (*Id.*). Defendants did neither.

First, Defendants failed to perform adequate searches. During the lead counsel conference, they couldn’t say whether they spent even one hour; earlier today, they suddenly reported to have spent “700 person hours.” Hours later, they claimed it was “500 person hours.” When pressed, they couldn’t substantiate either assertion. Either way, the searches were deeply flawed:

- Defendants failed to inspect any of the computers identified in Cadence’s phone-home reports. Worse yet (discussed below), they have been ***destroying*** computers—including some while the Dec. 22 motion was pending. They contend others have now been “reformatted,” and they haven’t inspected those, either.
- Syntronic AB and Beijing imposed arbitrary limitations—*e.g.*, only searching computers with a “last log on date ***within 180 days***” and limiting the search to China, Europe, and Canada, even though they also operate elsewhere. This search would not capture any computers Defendants took offline when this litigation was filed, much less from the years before. Syntronic USA has not said how far back its searches go. Defendants then promised to broaden their search and report back today—and failed (again) to do that. And the results

provided do not even capture computers that continue to report unauthorized use on Defendants' network, raising serious questions.

- Defendants also **refuse** to comply with 1(b) and (c) of the Order, which directs them to search computers of certain current / former employees' computers. (Dkt. No. 86 at 1; *see* Ex. C at 5 (limiting search to "engineers' company computers")). As the Court may remember, Defendants argued that some of computers appearing in phone-home reports belonged to their employees. During the lead counsel meet-and-confer, counsel admitted they made no effort to access even specific employee computers appearing in phone-home reports.

Second, Defendants failed to "fully respond" to Rogs 1-3. Their counsel disclosed that their clients **refuse** to provide this foundational discovery ordered by the Court, such as hostnames and IP addresses for offending machines (Rog 1), the identity of individuals who caused Cadence Software to be installed (Rog 2), and the requested identifying information for the users of these machines (Rog 3). Defendants' counsel acknowledges that witnesses have been interviewed (some of whom admitted to using the pirated software), but Defendants refuse to disclose responsive information. The following summarizes missing information required by the Court's Order:

Rog	Omitted Information (<i>See</i> Exs. A-C)
1	Hostname, IP addresses, and location of all identified machines. (<i>See</i> Ex. A at 27-28).
2	Facts and circumstances surrounding installation, date of installations, identity of Persons causing Cadence Software to be installed, and origins of the installed Cadence Software.
3	Identifying information for all users (Defendants often identified users as "Engineers"), full legal names, nicknames, other aliases, address, job titles and job descriptions.

Acknowledging their failure to comply, Defendants now "propose" that comity with foreign laws somehow excuses their noncompliance. That contention is wrong, but even setting aside the merits, it was incumbent on Defendants to raise any objections **before** their responses were due. At a minimum, they were required to seek reconsideration (before Your Honor or Judge Illston) instead of simply refusing to comply with an Order—especially since they had 45 days to comply. They did neither—they just ignored the Order and destroyed the computers. Even on the merits, Defendants fail to explain (either here or anywhere else) how foreign laws supposedly block the ordered discovery. Defendants are willfully failing to comply, and the Court should enforce the prior Order requiring them to do so.

Third, two months ago, the Court ordered the parties to agree on a "deadline for completion of document production by defendants." Defendants refuse to do so. They suggest below (untruthfully) that they "offered numerous dates-certain"—but **still** don't propose any concrete date in this letter or otherwise. Nor have they suggested that the 1,000 documents promised below for today would substantially complete that production. On the contrary, since the last hearing, Defendants have raised new objections—*e.g.*, on March 14, Defendants identified for the first time 13 RFPs that they claim may "implicate" foreign laws. (Ex. G; *see* Ex. H (no mention of GDPR)). Defendants' prior responses never raised these objections, and they are waived. *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1473 (9th Cir. 1992). Even now, Defendants have not explained how foreign law applies to any RFP even though "[t]he party relying on foreign law has the burden of showing that such law bars production." *United States v. Vetco Inc.*, 691 F.2d 1281, 1289 (9th Cir. 1981). The Court should order defendants to produce all documents responsive to all of Plaintiff's RFPs by April 14 or some other date certain.

Court's March 3 Order re Rog 10. To avoid another motion to compel, on March 2, Defendants stipulated to answering Cadence's Rog 10 by March 21, which the Court ordered on March 3.¹ (Dkt. Nos. 93-94). This interrogatory relates to infringing machines identified by Cadence in early 2020. Defendants previously claimed (*e.g.*, in sworn interrogatory responses and responses to a Notice of Inspection) that these machines were "cycled out" of use prior to February 2020 when Cadence gave notice of its claims. But Defendants refused to explain any details, so Plaintiff served Rog 10. (Exs. D-F). Defendants failed to comply with the Court's Order.

Before addressing what these responses *lack*, it bears mentioning what they *include*. Astonishingly, Defendants now admit to the most serious of discovery violations—the computers identified by Cadence were not "cycled out" of use before February 2020 (as they previously stated under oath). Rather, after receiving Cadence's Feb. and April 2020 notices, Defendants destroyed or "disposed" of at least 18 of these machines. ***At least seven were "disposed" on January 24, 2022 after Plaintiff filed its December 22 motion to compel.*** The remaining 24 machines were "reformatted" (*i.e.*, erased). Plaintiff has asked for more information on this spoliation and is evaluating a motion for sanctions, which it will raise separately.

Turning back to ***Rog 10***, Defendants still failed to provide the required information. For example, they *refuse* to identify all persons involved in "cycling out" these computers. (Ex. D). For the 24 "reformatted" computers, Defendants have not disclosed *when* they erased the data on those hard drives, their last known location, or to whom they were given. (*Id.*) And although they stipulated to an Order confirming "they will not withhold any information on the basis of any objections," (Dkt. Nos. 93-94), they are now trying to raise *new* objections. (Ex. D at 4 (adding cursory Chinese law objection in March 21 supplemental response)), and their counsel confirmed (at the lead counsel conference) that their clients refuse to provide information. Plaintiff asks the Court to enforce its prior Order requiring Defendants to provide all information within 10 days.

Defendants' Portion

Defendants complied with the Court's February 4, 2022 Order. Syntronic AB and Syntronic Beijing searched more than **800** computers across the entire Chinese, European, and Canadian network domains. Ex. B, 4:7-20. Approximately 130 computers had Cadence Software. Critically, ***not one of them*** contained an ***unauthorized*** version of Cadence Software. Ex. B, p. 17-30. Instead, all versions were either fully licensed (and Defendants identified the license) or free versions. *Id.* Syntronic USA conducted a search of its computers. Ex. C, 3:15-18. Not one of them contained Cadence Software. *Id.* Defendants invested many hundreds of hours (they roughly estimate in excess of **500 person hours** globally including the supplemental search) to capture, as reasonably and practicably as possible, all computers likely to contain Cadence Software and to provide responsive information. Not surprisingly, the results of this search are consistent with Plaintiff's own "phone home" data—Defendants are not now and never have been engaged in wide-spread software piracy. The only "evidence" of alleged unauthorized use is anomalous data in Plaintiff's "phone home" reports, isolated to China primarily in the 2017-2019 timeframe and driven by approximately just 12 computers. Future discovery should be focused accordingly.

Defendants agreed to conduct a supplemental search. Plaintiff did not like the results. On March 30, 2022, the parties held a lead trial counsel meet and confer. Plaintiff objected to two

¹ In January, Defendants agreed to answer Rog 10 and Cadence's Second Set of RFAs by February 11. Then, at 7:47 PM on the day those responses were due, Defendants announced that the promised discovery was not coming and refused to say when they would provide responses.

search terms: (1) the geographic scope; and (2) the use of a 180-day last logon date. Defendants explained the use of both terms. The search was limited to China, Europe, and Canada (and the US since Syntronic USA is a defendant) because those are the only locations where employees would utilize electronic design automation software, such as Cadence Software. The use of a 180-day last logon date was to capture the likely universe of searchable computers connected to the network. Plaintiff rebuffed those explanations. Plaintiff also complained about certain information on how the Cadence Software was downloaded. Defendants explained that some of that information simply was not available through the network search. Plaintiff balked and demanded the information nonetheless. So, to avoid further dispute, and notwithstanding the additional cost and low likelihood that it would yield different results, Defendants agreed to conduct a supplemental search on those issues and agreed to update Plaintiff the following week.

Plaintiff refused to wait. Two days later, on Friday, April 1, it sent a draft letter and demanded Defendants' portion by Tuesday. On Tuesday, Defendants confirmed the supplemental search was under way, but it required coordination across multiple countries, so they anticipated results by the weeks' end. Plaintiff refused to wait. If it did not receive Defendants' portion by Wednesday, Plaintiff threatened to "proceed unilaterally." Rather than burden the Court with competing letters, Defendants agreed to participate in a joint letter, but they will serve supplemental responses based on the supplemental search, likely mooted some of these issues.

The Court did not order Defendants to individually search its employees' computers. The Court ordered Defendants to search computers owned by current or former employees "used . . . in the course of their employment[.]" Dkt. No. 86. Defendants' search accounted for that. As a practical matter, if an employee used a personal computer for work, the employee would have logged onto one of the networks. Defendants' search of over 800 computers included every computer that logged onto a network and is still reachable through a network search. If one of those computers was an employee's personal computer, it was searched.

The Court did not order Defendants to physically inspect all computers that may have historically connected to Defendants' networks. One of the reasons the Court accepted Plaintiff's argument that Defendants should be forced to search unnamed affiliates, despite the fact Plaintiff has absolutely no evidence of their unauthorized usage, is because the Court concluded that there was evidence that all of the affiliates operated on "one network." Feb. 4, 2020 TR., 16:12-14. They do not, in fact, operate on one network, but the Court appears to have correctly had in mind that Defendants could perform some type of network search that did not require the burdensome physical inspection of all computers. Defendants did exactly that. But it is neither reasonable nor practical for Defendants to seek out and physically inspect all computers that may have historically connected to the network, particularly *without any evidence* – in Plaintiff's "phone home" spreadsheets or otherwise – that they ever contained Cadence Software. The Court made clear that it was "expecting the plaintiff to be very circumspect about how much it needs . . . and not overdo it." Feb. 4, 2020 TR, 22:1-3.

Defendants' respectfully propose that comity prohibits them from disclosing personal identifying information. Defendants *did* produce names and personal identifying information for engineers in Canada, and Defendants *did* produce brand/model information as well as geographic location. Exs. A, pp.18, 27-28; B, p.17-30. However, Syntronic AB and Syntronic Beijing objected to providing personal identifying information, such as user names, IP addresses, and personal names and addresses, under the General Data Privacy Regulation (GDPR) and Chinese data and privacy laws. Far from waiving these objections, Defendants objected and put Plaintiff on notice in October and February. Exs. J, I. They subsequently retained local counsel in their home

countries to advise them. Their concerns are not trivial. Even “lower level” sanctions under GDPR can result in fines up to €10 million, or 2% of annual revenue, whichever is *higher*.² Companies face similar sanctions under Chinese law, including up to CNY50mm (~\$7mm) or 5% of annual revenue.³ Moreover, GDPR enforcement has recently increased significantly, jumping from 16 fines in 2018, to ~302 fines in 2020 and ~266 fines in 2021.⁴

The Supreme Court has long recognized that “American courts should therefore take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state.” *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa*, 482 U.S. 522, 546 (1987). Defendants acknowledge this Court is not bound by GDPR or Chinese law, but Syntronic AB and Syntronic Beijing indisputably are. Comity should afford them at least the opportunity to object to requests that would require them to risk violating their home countries’ laws. *See AnyWhereCommerce, Inc. v. Ingenico, Inc.*, 2020 WL 5947735, at *1-2 (D. Mass. Aug. 31, 2020) (“the GDPR may be fairly construed as an objection by a foreign state over some of the discovery sought by Plaintiffs To that end, comity towards France may be implicated and the court is obliged to consider the factors set forth by the Supreme Court—and any other considerations that may be relevant—before compelling the discovery sought here.”).

Importantly, none of the more than 800 queried computers contained unauthorized versions of Cadence Software. Personal identifying information on those computers therefore bears no proportional relevance to Plaintiff’s claims. Additionally, Cadence has the MAC addresses for each of the relevant computers, and it does not truly need personal identifying information to confirm that those computers did not use unauthorized software. Feb. 4, 2020 TR, 22:1-3 (“expecting the plaintiff to be very circumspect about how much it needs . . . and not overdo it.”).

Plaintiff rejected Defendants’ offers for a date-certain production. The parties met and conferred and Defendants offered numerous dates-certain. Plaintiff rejected them all and would not agree unless conditioned on other issues outside of the Court’s order. Regardless, on April 6, 2022, Defendants produced approximately an additional 1,000 documents, which they anticipate should substantially complete at least what Syntronic USA and Syntronic AB agreed to produce in response to RFPs, Set One. The same is true for Plaintiff’s RFPs, Sets Two and Three, even though those requests were not before the Court on February 4, 2022, and Plaintiff has never sought to meet and confer on a single one of Defendants’ responses. Pursuant to Standing Order, Section E.11, they will supplement their responses in light of the production to identify and confirm the documents that have been produced. If any outstanding documents they agreed to produce remain, and subject to their objections (which remain unchallenged), they will produce them promptly.

Syntronic Beijing adequately responded to Interrogatory No. 10. Syntronic Beijing identified its general computer recycling practices and produced the policies governing those practices. It then identified, to the extent it was able, when, why, how, and generally the persons to whom the computers were conveyed, as Interrogatory No. 10 requested.

² <https://gdpr.eu/fines/>

³ <https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection>

⁴ <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement>

Best regards,

/s/ Steve Papazian

Guy Ruttenberg
Steve Papazian
Ruttenberg IP Law, A Professional Corp.
Attorneys for Cadence

/s/ Jason N. Haycock

Edward P. Sangster
Jason N. Haycock
K&L Gates LLP
Attorneys for Defendants

ATTORNEY'S E-FILING ATTESTATION

As the attorney e-filing this document, and pursuant to Local Rule 5-1(h)(3), I hereby attest that counsel for Defendants whose electronic signature appears above has concurred in this filing.

/s/ Steve Papazian

Steve Papazian
Ruttenberg IP Law, A Professional Corp.
Attorneys for Cadence